Type of submission:	Paper
Title:	Security Proof of Concept Keystone (SPOCK)

Abstract:

SPOCK is a joint government and industry consortium sponsored by the National Security Agency to demonstrate security features of commercial and government products that can support dependable security architectures. The activity provides a forum for government users and security technology providers to share information on security requirements, emerging technologies, and new product developments. Integrators and product developers are afforded opportunities to share new solutions, identify government developed technology available for commercial use, and prototype COTS products in government sponsored test beds.

Author:	James McGehee and James R. Reid
Organizational Affiliation:	COACT. Inc.
Phone / FAX :	(301) 498-0150 / (301) 498-0855
E-mail address:	jom@coact.com
Point of Contact:	James McGehee
U.S. Government Sponsor:	NSA/V2
Contract number:	MDA 904-96-C-0215
Publication Release Authority:	NSA/V2

SPOCK

SECURITY PROOF OF CONCEPT KEYSTONE

James McGehee
COACT, Inc.
9140 Guilford Road, Suite L
Columbia, Maryland 20146

In 1992 representatives from the vendor community and National Security Agency believed that emerging security products could provide some security solutions within a given architecture. The goal of the group was to seek out security products and demonstrate their usefulness within government system architectures. This goal was the keystone for the established program called Security Proof-of-Concept Keystone (SPOCK).

The SPOCK program is a joint government and industry forum sponsored by the National Security Agency to demonstrate security features of commercial and government products that can support dependable security architectures. The activity provides a forum for government users and security technology providers to share information on security requirements, emerging technologies, and new product developments. Integrators and product developers are afforded opportunities to share new solutions, identify government developed technology available for commercial use, and prototype commercial-off-the-shelf products in government sponsored test beds. The SPOCK forum meets monthly to share information about emerging architectures, secure products, security requirements, threats, standards and building codes. SPOCK members include representatives from the National Security Agency, military services, government services, including agencies outside of the Department of Defense, and industry to include integrators, and product developers. Product developers, contractors and test bed clients participating in SPOCK initiatives are permitted and encouraged to volunteer time, materials, and personnel according to the perceived value of the initiatives. To be a member and to participate in the group, representatives from government and industry organizations should have security awareness, be involved in communications products or services (including software), understand that security integration does affect change in products and services, be an individual or organization who targets Information Security as a necessary technology, and be willing to share information and resources to improve our knowledge base and ability to implement security products.

The purpose of SPOCK is to:

a) Demonstrate that current certified products can provide a measure of systems security.

b) Determine if any uncertified system components can be used to improve a secure system.

c) Define products that can support secure architectures.

d) Define the risks in using these secure architectures.

e) Showcase technology--not develop it

The group has developed a capability to do testing and proof-of-concept demonstrations on products within given architectures both in the laboratory and in operational network settings. The proof-of-concepts are designed to independently verify the accuracy of vendor claims about the security of their products.

The SPOCK program makes use of existing laboratories and contract vehicles. It provides a forum for government and industry to have a continuing dialogue toward solving network security requirements. In addition to testing and proof-of-concept demonstration opportunities, it also provides an archive of completed proof-of-concept reports on system architectures and products with security features and policy for members and network architects to use. At the monthly meetings briefings are given by government representatives that describe architectures, requirements, or new government developed security technology. From commerce representatives, briefings are presented on new security products, implemented security architectures, or commercial sector requirements.

SPOCK participation is voluntary. The focus is Information Security. Presentations and proof-of-concepts are proposed and presented by any participant.

Presentations and proof-of-concepts are proposed by the forum membership. A proof-of-concept demonstration begins with identification of Vendor Claims and a sponsored architecture to be tested. When a proposed proof-of-concept is accepted by the SPOCK Chairman (a National Security Agency member), a team is formed. This team is composed of volunteer forum members who are interested in the proof-of-concept or who can contribute resources (i.e. technical support, hardware, software, test equipment, connectivity, etc.). A test plan is written and agreed to by all participants in the proof-of-concept demonstration. The test plan focuses on the vendors claim package. In addition, performance tests are applied when possible. The SPOCK integration contractor coordinates support between team players, supervises the demonstration and test activities and publishes the final test report. A draft report is written, reviewed by the test team and approved by the SPOCK chairman. The report is then published and distributed to interested participants. All of the reports are controlled. They are not classified. SPOCK reports can be requested through the integration contract:

COACT, Inc.
9140 Guilford Road, Suite L
Columbia, Maryland 21046
Phone: 301-498-0150
Fax: 301-498-0855

The following are some examples of proof-of-concept test plans and reports:

1). BLACKER Front End LAN, Document No.1600383, 14 December 1993

2). Raptor, Eagle/Eaglet Test Plan, Document No. 1600390, October 1993

3). Raptor Eagle/Eaglet, Test Report, Document No. 1600393, February 1994

4). Filter Router Test Plan - Phase I, Document No. 1600386, November 1993

5). Filter Router Test Report, Executive Summary, Document 1600411, April 1994 (3COM, Alantec, CISCO, Network Systems, Proteon, and Wellfleet)

6). Buttress Test Report, Document No. 1600424, 13 June 1994 (a successful joint Air Force, Navy, Sprint, SPOCK initiative to provide off-board imagery and emitter information to an aircraft in a timely fashion to support targeting of non-line-of-sight targets for tactical air strikes)

7). Network Security Router, Performance and Security Test, Document No. 10504, 29 March 1996

The latter was the most recent proof-of-concept conducted by the SPOCK Program to validate vendor claims of performance and security goodness of the Network Systems Corporation's, Security Router. Participants in the proof-of-concept were the Air Force Space Command Space Warfare Center, the Army Battle Command Battle Laboratory, the Internal Revenue Service, NSA/V2, NSA/Y4, Network Systems Corporation, and COACT,Inc. The Internet was used as a connecting medium between the test nodes. Performance testing and mandatory access control (MAC) testing was performed at and by the IIT Research Institute (an Internal Revenue Service federally funded research and development contractor). Penetration testing was conducted by

NSA/C44 personnel. The tests were monitored by SPOCK participants. The result of tests performed showed that when configured properly, the router would provide highly reliable and secure communications across an unsecured network, and that data could be passed at speeds in excess of 1 Mbps. Applied attempts to penetrate the network from outside of trusted enclaves were unsuccessful. The following is an example of Vendor Claims.

EXAMPLES OF VENDOR SECURITY CLAIMS

Network Attack Protection

Selectively permit traffic through the router
Protect against IP level spoofing
Provide audit of attack violations
Prevent and audit unauthorized protocols
Prevent and audit unauthorized network service applications
Prevent and audit fragments from entering networks
Prevent and audit source routed packets

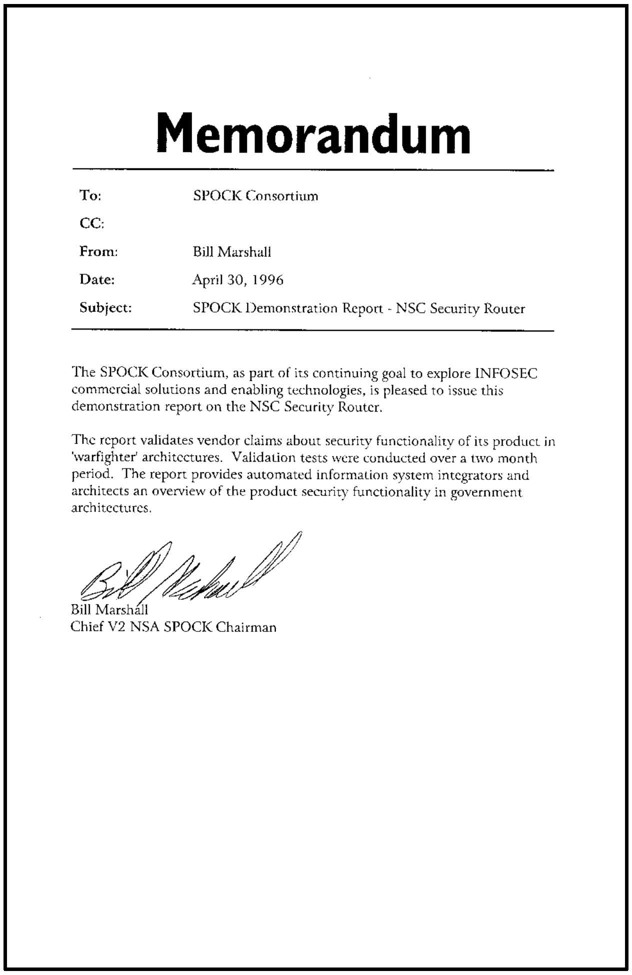
Data Privacy

Encrypts data transmitted by the router at 1 Mbps
Prevents access to public key information during exchange
Detect and audits replay attacks
Authenticates communicating routers

Mandatory Access Control

Selectively allows traffic based on RIPSO labels
Assign default labels to unlabeled datagrams
Routes datagrams based on RIPSO labels
Encrypts datagrams based on RIPSO labels

As a result of completing a proof-of concept under the auspices of SPOCK, a Memorandum is issued and signed by the Chief of NSA/V2 as the SPOCK Chairman.



Memorandum

To:	SPOCK Consortium
CC:	
From:	Bill Marshall
Date:	April 30, 1996
Subject:	SPOCK Demonstration Report - NSC Security Router

The SPOCK Consortium, as part of its continuing goal to explore INFOSEC commercial solutions and enabling technologies, is pleased to issue this demonstration report on the NSC Security Router.

The report validates vendor claims about security functionality of its product in 'warfighter' architectures. Validation tests were conducted over a two month period. The report provides automated information system integrators and architects an overview of the product security functionality in government architectures.

Bill Marshall
Chief V2 NSA SPOCK Chairman

At each monthly SPOCK meeting, discussions, briefings and sharing information takes place. The following are examples of previous presentations:

a) Common Criteria (V2)

b) Sterling Software Secure Network (Sterling)

c) DirecPC (Hughes Information Technology Systems)

d) Shipboard Network Integration (Lockheed/Martin)

e) Dockmaster II

f) C4 Attack Center (C44)

g) MISSI Certificate Architecture (NSA/X33)

h) NSC Secure Router (NSC)

i) ATM Networking (NSC)

j) Virtual Campus (NSA/Y44)

k) Pathkey (Paralon)

l) Joint Interoperability Test Center Capability (JITC)

m) Joint Warfighter Interoperability Demonstrations (NSA/V2)

n) INFOGUARD, ATM Cell Encryptor (Cylink and GTE)

For efficient response to proof-of-concept proposals, SPOCK takes advantage of existing laboratories and networks. These resources can be in government or commercial sites. Current sites are the Space Warfare Center at Falcon Air Force Base, Colorado, the Army Battle Command Battle Laboratory at Fort Gordon, Georgia, IITRI in Lanham, Maryland., and the National Security Agency at Fort Meade, Maryland.

An important segment of the SPOCK program is its commitment to support the Warfighter effort. SPOCK has been introduced to the Joint Warfighter Interoperability Demonstration (JWID) program managers. Discussions are continuing on ways for SPOCK to support the JWID demonstrations.

It should be noted that the SPOCK program is not intended to, nor does it compete with programs such as the Trusted Computer Security Evaluation Criteria (Orange Book), the Common Criteria Program, the National Institute of Standards and Technology initiatives and programs, or the Multilevel Information Systems Security Initiative. SPOCK supports these formal type of initiatives by providing data that gives customers, developers and evaluators an early view of the product/system security attributes. This data can support decisions by the customer as to whether the system fulfills or has potential to fulfil their security needs. This data helps the developer determine the state of his security functions and assurances. It can help the developer determine whether the product is ready to proceed with a formal evalaution or does it need more tweaking. Finally, this data can support the evaluator when forming judgements about the conformance of the product/system to targeted security requirements.

SPOCK provides a low cost, and quick look at security products within a specific architecture. The SPOCK proof-of-concept reports provide empirical information to network architects and accreditors. This data can help them to make informed decisions concerning their architectures and products that can be effectively used in their architectures. Some valued added features of the SPOCK Program include:

a) Evaluated, certified, or endorsed products can be prototyped in test bed configurations that may be different from those for which the product was originally reviewed.

b) Products can be prototyped to determine the usefulness of uncertified or untrusted products and solutions in client architectures.

c) Information Security products, processes, policies and technologies can be reviewed in test architectures.

d) Test beds can be used to prototype innovative Information Systems Security Engineering (ISSE) techniques.

e) Independent validation of Product developer claims

f) Supports accreditation and certification initiatives

SPOCK continues to focus on emerging security technologies. Vendor claims have been received for the IRE Fortezza Modem (Industrial Research Engineering), and the INFOGUARD ATM Cell Encryptor (Cylink and GTE). Development of test architectures and test plans are on-going. Other potential proof-of-concepts include the Network Systems ATM Encrypting Router, and the DirecPC (Hughes Information Technology Systems) which provides a global broadcast capability to include encryption.

In summary, SPOCK has been successful. The monthly meetings and the proof-of-concept demonstrations have provided useful information to the vendor for design, development and product improvements. The developers of security products have the opportunity meet potential customers. Integrators have the opportunity to learn about new products for security solutions. The SPOCK customers such as accrediting authorities have been provided valuable data needed to assist in making decisions about security products usefulness.

References:

1. SPOCK CONCEPT OF OPERATIONS, Document No. 5400001, Revision 7, August 1995